NASA Policy Directive

NPD 2810.1E
Effective Date: July 14, 2015
Expiration Date: July 14, 2020

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Information Security Policy

Responsible Office: Office of the Chief Information Officer

NASA Interim Directive (NID): Use of NASA Information and Information Systems while Outside of the U.S. and Territories, NID 2810.107A

1. POLICY

a. This NASA Policy Directive (NPD) consolidates information security policy for both classified and unclassified information. Responsibility for information security is shared between the Office of the Chief Information Officer (OCIO), which is responsible for unclassified information, and the Office of Protective Services (OPS), which is responsible for classified information.

b. NASA's policy is to:

(1) Protect all NASA information and information systems, both classified and unclassified, in a manner that is commensurate with the national security classification level, sensitivity, value, and criticality of the information.

(2) Protect NASA information from unauthorized disclosure, destruction, or modification while the information is being collected, processed, transmitted, stored, or disseminated.

(3) Manage the security of all classified and unclassified Information Technology (IT), through the complete system development life cycle, that is acquired, developed, or used in support of NASA missions, programs, projects, and institutional requirements.

(4) Manage the security of all information systems in a cost-effective manner, guided by the application of sound risk management processes that ensure a level of confidentiality, integrity, and availability of information in each phase of the system development life cycle.

(5) Conduct periodic assessments and reviews to verify compliance with this directive and other applicable Federal and NASA policies that process, store, or transmit NASA data.

(6) Investigate information security incidents through incident management and forensic investigation, and develop after action reports following significant incidents to address security issues and improve future response efforts.

(7) Ensure information security policy requirements, audits, and forensic investigations are implemented across Centers and contracts.

(8) Implement security policy best practices and guidance outlined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series and Federal Information Processing Standards (FIPS).

(9) Ensure all unclassified information systems operating within the NASA environment are operating under a valid authority to operate, and that all classified information systems operating within the NASA environment are operating under a valid System Security Authorization Agreement.

2. APPLICABILITY

a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the contracts, grants, or agreements.

b. This NPD is applicable to all NASA users of IT (e.g., civil servants and contractors) when supporting Agency projects, programs, and missions.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

a. Inspector General Act of 1978, as amended, 5 U.S.C. App. III.

b. Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

c. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101 et seq.

d. Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541 et seq.

e. Federal Information Security Management Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq.

f. E-Government (e-Gov) Act of 2002, as amended, 44 U.S.C. § 3601 et seq.

g. National Aeronautics and Space Act, 51 United States Code (U.S.C.) § 20101 et seq.

h. Executive Order (EO) 13526, Classified National Security Information, as amended (December 2009).

i. Office of Management and Budget Circulars (Generated by OMB) - OMB Circular A-130.

j. Office of Management and Budget Memorandum (Generated by OMB) - Memorandum, M-11-33.

4. APPLICABLE DOCUMENTS AND FORMS

a. NPD 9800.1, NASA Office of Inspector General Programs.

b. NPR 1600.3, Personnel Security.

c. NPR 1600.1A, NASA Security Program Procedural Requirements.

d. NPR 2810.1, Security of Information Technology.

e. NIST SP 800 Series. (URL: http://csrc.nist.gov/publications/nistpubs/index.html).

f. Federal Information Processing Standards (FIPS). (URL: http://csrc.nist.gov/publications/fips/index.html).

5. RESPONSIBILITY

a. The NASA Administrator (or designee) shall:

1. Provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of NASA within information systems used or operated by NASA, by a NASA contractor, or another organization on behalf of NASA.

2. Comply with the requirements of Federal Information Security Management Act (FISMA) and other Federal laws, related policies, procedures, standards, and guidelines on unclassified information security and national security systems (i.e., classified systems).

3. Ensure that information security management processes are integrated with NASA's strategic and operational planning processes.

(a.) Ensure that senior NASA officials provide information security for the information and information systems that support the operations and assets under their control through:

(1.) Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

(2.) Determining the levels of information security to protect such information and information systems for information security classifications and related requirements, and providing the adequate information security resources to do so.

(3.) Implementing policies and procedures to cost-effectively reduce risks to an acceptable level.

4. Periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

5. Allow only those information systems that are determined not to pose an unacceptable risk to NASA information, missions, programs, projects, and institutional requirements.

b. The NASA CIO shall:

1. Ensure compliance with the information security requirements imposed on NASA.

2. Develop and maintain an Agency-wide information security program. This program will be accomplished by establishing and implementing information and information system security policies and procedures, and by issuing instructions, memoranda, handbooks, and bulletins designed to facilitate protections.

3. Designate a Senior Agency Information Security Officer (SAISO).

4. Ensure the development and maintenance of information security policies and procedures to protect unclassified information, and ensure that sufficient resources are allocated to address information and information system security requirements developed under this directive.

5. Ensure the development and maintenance of a security assessment and authorization program compliant with the Federal Information Processing Standards (FIPS), and National Institute of Standards and Technology (NIST), Special Publications (SP) 800 Series for ongoing authorization and continuous monitoring of Federal information systems.

6. Designate, for unclassified information systems, the Agency organization positions for Authorizing Officials (AO), establish AO requirements, and approve the individual AOs who shall have the authority, accountability, and responsibility for system risk to Agency operations in accordance with NIST SP 800-37.

7. Appoint an Enterprise Services Security Integration Lead with responsibility for coordinating with the OCIO Enterprise Service Office Security Leads to provide unified and integrated security representation for the OCIO Enterprise Service Offices. The security managers within each Enterprise Service Office will work with the Enterprise Services Security Integration Lead to coordinate and provide consistent security reporting, incident coordination, risk analyses, etc. The Enterprise Services Security Integration Lead will be a full voting member on the IT Security Management Board (ITSMB) and will provide input, analysis, and recommendations on behalf of OCIO Enterprise Services.

8. Train and oversee personnel with responsibilities for information security.

9. Issue procedural requirements updates regarding protection and management of unclassified information and information systems in the form of a NASA Information Technology Requirement (NITR) to keep pace with the dynamic information security environment.

10. Establish and maintain a NASA Security Operations Center (SOC) to provide consolidated unclassified information security operations and incident response capability that provides Agency-wide visibility and monitoring of NASA networks and systems.

11. Ensure procedures are established for the referral of suspected and confirmed incidents involving unclassified information systems to the NASA Office of the Inspector General (OIG) for investigation in a timely manner. Computer crimes may include, but are not limited to:

(a) Unauthorized information.

(b) Compromises of computers.

12. Coordinate the initial assessment of suspected computer crimes related to unclassified information or information systems, such as unauthorized access of information, compromises of computers, and other information systems, such as telecommunications systems, command and control systems, and network systems, with the Office of Inspector General (OIG), and other organizations or agencies.

13. Establish a NASA information security capability for unclassified information and information systems with the mission and resources to:

(a) Develop and implement an information security review program designed to ensure that all NASA information systems used to process unclassified information are in compliance with NASA policy, NASA procedural requirements, and Federal guidelines and statutes, ensuring that security reviews are coordinated with the NASA Office of Inspector General to minimize duplicative review efforts.

(b) Be responsible for the investigation of sensitive information (e.g., Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) security incidents.

(c) Support counterintelligence reviews, threat assessments, and investigations and issue NASA threat bulletins to protect unclassified information.

14. Charter an ITSAB to advise the NASA Information Technology Management Board (ITMB), the SAISO, and the NASA IT community on information security issues.

c. The NASA Assistant Administrator for Office of Protective Services (OPS) shall:

1. In collaboration with the NASA CIO, establish a program with multiple security disciplines (e.g., physical, personnel, industrial, communications security (COMSEC), and emanations security (TEMPEST) for the oversight and protection of Classified National Security Information (CNSI) to include security control assessments and security authorizations of national security systems in compliance with the national security authorization process.

2. Establish a NASA COMSEC Material Control System (CMCS).

3. Appoint a Central Office of Record (COR) which shall:

(a) Set forth minimum National Security Agency requirements, standards, procedures, specifications, and guidelines for safeguarding and controlling COMSEC material in NASA's possession.

(b) Investigate and monitor COMSEC incidents.

4. Coordinate the initial assessment of suspected computer crimes related to classified information and information systems with the NASA CIO, the OIG, and other organizations or agencies. Computer crimes include:

(a) Unauthorized access of information.

(b) Compromises of computers.

(c) Compromises of information systems such as telecommunications systems, command and control systems, and network systems.

5. In accordance with NPR 1600.3, Personnel Security, establish policy and procedural requirements for security background investigations of persons who require access to IT systems, applications, and networks operated by or on behalf of NASA.

6. Conduct counterintelligence reviews and threat assessments and investigations, and issue threat bulletins for NASA to protect both classified and unclassified information and information systems.

7. Provide input to the NASA CIO regarding threat assessments for unclassified information systems.

8. For classified information security incidents, be responsible for investigation of the information security incidents, cooperate and assist (as requested) with the OIG in its investigation of information and information system security incidents, and refer to the NASA Counterintelligence Director classified security incidents with a counterintelligence nexus.

9. Ensure that sufficient resources are allocated to address information and information system security requirements developed under this directive for OPS information systems.

d. The Associate/Assistant Administrators for Mission Directorates shall:

1. Participate with the NASA CIO and the Assistant Administrator for OPS in their respective development of NASA information security policies, standards, best practices, and guidance that protects NASA information and information systems.

2. Appoint an IT Security point of contact to represent the mission on Agency programmatical strategic security initiatives and serve as voting members of the ITSMB.

3. Ensure that sufficient resources are allocated to address information and information system security requirements

developed under this directive for their information systems.

4. Ensure that their respective organizations, including missions, programs, projects, and institutions under their purview, comply with this directive.

5. Ensure that adequate information security risk management design and planning is conducted to allow for effective cost-benefit analyses of alternate information security postures and of risk acceptance.

e. The OIG shall be responsible for the investigation of all computer security crimes, such as unauthorized access of information systems, compromises of computers and other information systems such as telecommunications systems, command and control systems, and network systems. (NPD 9800.1, NASA Office of Inspector General Programs.)

f. The Mission Support Offices shall:

1. Apply these policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software (e.g., IT in spacecraft, aircraft, satellites, facility and system monitoring equipment, and test equipment to include uplink, downlink, and crosslink command and communications) throughout the system life cycle and for other embedded IT, through design, development, test, and evaluation, until and through decommissioning.

g. The SAISO shall:

1. Carry out the Agency CIO's responsibilities for information security.

2. Possess professional qualifications, including training and experience, required to administer the functions described under this section.

3. Be responsible for information security duties.

4. Establish an office with the mission and resources for information security operations, security governance, security architecture and engineering, and cyber-threat analysis to assist in ensuring Agency compliance with Federal information security laws, directives, policies, standards, and guidelines.

5. Manage the Agency's information security program and activities for unclassified information and information systems, including the preparation and maintenance of NPR 2810.1, Security of Information Technology.

6. Provide program management of the Agency's unclassified information security programs and projects.

7. Serve as the NASA Information System Risk Executive, related to NIST requirements, responsible to ensure that security risk-related considerations and risk management of individual information systems are consistent across the Agency, are viewed from an Agency-wide and strategic goal perspective, and reflect the Agency's information system risk tolerance affecting mission/business success.

8. Establish and manage the Agency information security performance metrics program.

h. The Center Directors and the Director for Headquarters Operations shall:

1. Ensure compliance with this directive, NASA policies, procedures, requirements, and the Federal information security policy for activities under their purview.

2. Apply these policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software throughout the system life cycle and for other embedded IT, through design, development, test, and evaluation, until and through decommissioning.

3. Designate a Center CISO in writing.

4. Notify the SAISO, in writing, of the Center CISO who will act as a Voting Member of the ITSMB.

5. Ensure the Center CIO has adequate staff, resources, budget, and authority to implement information security programs at their Center.

6. Make available qualified personnel to support periodic security assessments conducted by the Agency OCIO.

i. The Center CIOs and the Headquarters CIO shall:

1. Be responsible and accountable for the protection of information and information systems under their purview.

2. Be responsible and accountable for compliance with this directive, NASA information security policies and procedures and the Federal information security laws, directives, policies, standards, and guidelines.

3. For unclassified security incidents, be responsible for the coordination of investigations of information security incidents to include:

(a) Notifying the NASA Security Operation Center of the information security incident.

(b) Referring an information security incident to an investigating authority.

(c) Cooperating and assisting the NASA OIG with its investigation of computer crimes, as requested.

(d) Referring information security incidents with a counterintelligence nexus to the NASA Counterintelligence Director.

j. The Center CISO shall:

1. Responsible for the implementation of IT Security policies to the Center CISO.

2. Assist the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws, directives, policies, standards, and guidelines.

3. Serve as the primary interface between the SAISO and Center information security functions.,/p>

4. Head a program with the mission and resources for information security operations, security governance, and security architecture and engineering to assist the Center CIO in the compliance with Federal information security laws, directives, policies, standards, and guidelines.

5. Serve as the Center's voting member of the Agency ITSMB.

k. The NASA IT User shall:

(1) Adhere to information security policies, processes, and procedures outlined by the NASA CIO, including security and awareness training requirements.,/p>

6. DELEGATION OF AUTHORITY

The NASA CIO is authorized by FISMA and other Federal information security laws, directives, policies, standards, and guidelines to ensure Agency compliance.

7. MEASUREMENT/VERIFICATION

a. The effectiveness of this directive will be assessed as follows:

(1) Measurements will be collected and evaluated by the NASA CIO to assess the effectiveness of this policy directive at least annually by measuring the degree of compliance with assignments of responsibility for information security, establishment of security plans, review of security controls, and documented ongoing authorizations that provide an indication that security plans are adequately implemented.

(2) Measurements will be collected and evaluated by the NASA CIO at least annually to assess trends involving information security incidents and trends for tracking metrics involving the cost, schedule impact, and effect on mission, program, and project performance attributed to the loss, alteration, unavailability, misuse, or unauthorized access to or modification of Agency information or information systems.

8. CANCELLATION

NPD 2810.1D, NASA Information Security Policy, dated May 9, 2009.

/s/ Charles F. Bolden

ATTACHMENT A: (TEXT)

Classified National Security Information (CNSI) - means information that has been determined pursuant to EO 12958, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Control -The exercise of NASA's authority to regulate access to information.

Information - Any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for or is under the control of NASA.

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [44 U.S.C., Sec. 3542].

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [44 U.S.C., Sec. 3502].

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources [40 U.S.C. § 11101 et seq., Clinger-Cohen Act of 1996].

National Security System - Any NASA information system designated as being authorized to process CNSI.

Unclassified Information - All information that does not meet the criteria described in EO 12958, as amended. Federal requirements for protecting unclassified information are prescribed in FISMA.

ATTACHMENT B: ACRONYMS

AO Authorizing Official

ATO Authorized to Operate

CIO Chief Information Officer

CISO [Center] Chief Information Security Officer

CMCS COMSEC Material Control System

CNSI Classified National Security Information

COMSEC Communications Security

COR Central Office of Record

CUI Controlled Unclassified Information e.g. exempli gratia (for example)

EO Executive Order

FIPS Federal Information Processing Standards

FISMA Federal Information Security Management Act

IT Information Technology

ITMB Information Technology Management Board

ITSMB Information Technology Security Management Board

JPL Jet Propulsion Laboratory

NASA National Aeronautics and Space Administration

NIST National Institute of Standards and Technology

NITR NASA Information Technology Requirement

NPR NASA Procedural Requirement

OCIO Office of the Chief Information Officer

OIG Office of Inspector General

OPS Office of Protective Services

SAISO Senior Agency Information Security Officer

SBU Sensitive But Unclassified

SOC Security Operations Center

SP Special Publication

SSAA System Security Authorization Agreement

U.S.C. United States Code

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.